REMARKS

Claims 24-37 are pending in the Application. In the Final Office Action, the Examiner rejected claims 24-37 under 35 U.S.C. § 103(a) as allegedly not being patentable over U.S. Patent No. 6,278,783 ("Kocher1") in view of U.S. Patent No. 6,327,661 to ("Kocher2"). Applicant respectfully requests reconsideration and withdrawal of the finality of the Office Action and the rejection of the claims for the reasons set forth below.[1]

Request for Withdraw of Finality

Applicant requests that the finality of the Office Action be withdrawn. M.P.E.P. § 706.07 states:

> Before final rejection is in order a clear issue should be developed between the examiner and applicant. ...While the rules no longer give to an applicant the right to "amend as often as the examiner presents new references or reasons for rejection," present practice does not sanction hasty and ill-considered final rejections. The applicant who is seeking to define his or her invention in claims that will give him or her the patent protection to which he or she is justly entitled should receive the cooperation of the examiner to that end, and not be prematurely cut off in the prosecution of his or her application. ... The examiner should never lose sight of the fact that in every case the applicant is entitled to a full and fair hearing, and that a clear issue between applicant and examiner should be developed, if possible, before appeal. (Emphasis added.)

Applicant appreciates the explanation of Kocher2 provided by the Examiner in response to Applicant's request for clarification of the previous rejection. (*See* Office Action, p. 2-4; Applicant's Response dated May 8, 2007, p. 3.) The previous Office Action, however, included no such explanation or detail - it simply repeated Applicant's claim language. (*See* Office Action, mailed February 8, 2007, pp. 4:21-5:7.) As such, Applicant could not have been reasonably expected to glean the Examiner's interpretation of Kocher2 from the previous Office Action. Accordingly, no clear issue has been developed between the Examiner and Applicant, and Applicant has not been given an fair opportunity to respond. The Examiner was, therefore, premature in making the rejection final in reply to Applicant's Response without amendment. To give Applicant a full and fair hearing, Applicant

[1] The Office Action contains statements characterizing the claims and related art. Regardless of whether any such statements are specifically addressed herein, Applicant's silence as to these characterizations should not be construed as acceptance of them.

respectfully requests that the Examiner reopen prosecution and issue an Office Action responding to this Request for Reconsideration.

Rejection Under 35 U.S.C. § 103(a)

Applicant traverses the rejection of claim 27 under Section 103(a) because the purported combination of Kocher1 and Kocher2 fails to disclose or suggest Applicant's claimed subject matter. The Examiner concedes that Kocher1 fails to disclose or suggest, amongst other claimed features, "executing [a] permutation operation on each of the first and second random values, to generate respective first and second random results," as recited in Applicant's claim 24. The Examiner looks to Kocher2 for its alleged disclosure of these features.

Kocher2 discloses a blinded randomized-order permutation operation including four steps: initialization, blinding, permutation, and unblinding. (Kocher2, col. 12:20-25.) In the blinding step, a random number generator produces a random blinding bit. (*Id.* at col.12:45-55.) A temporary buffer (temp) is initialized with an XOR of the random bit and an input data bit, where the input data bit is selected according to a table (perm) constructed previously. (*Id.*) Additionally, an output buffer (dataOut) is initialized with the blinding bit, where the dataout bit is the result of using the input permutation table to operate on the index to temp. (*Id.*) In the permutation step, input bits are loaded in the order specified by the table (perm), permuted according to an externally-specified permutation table (table) and XORed onto the destination table (dataOut). (*Id.* at col. 12:56-60.)

The Examiner apparently asserts that Kocher2's random binding bit b, temporary buffer (temp), output buffer (dataOut) and table (perm) correspond to Applicant's claimed "first random value," "second random value," "first random result," and "second random result," respectively. (Office Action, pp. 3-4.) In addition, it appears that the Examiner asserts that the blinding step and the permutation step correspond to Applicant's claimed

"executing [a] permutation operation on each of the first and second random values, to generate respective first and second random results." (*Id.*) Applicant disagrees.

Kocher2's blinding step and permutation step are different steps for performing different operations on their respective inputs. The blinding step initializes the output buffer (dataOut) with the blinding bit b. (Kocher2 at col.12:45-55.) Differently, the permutation step loads input bits in the order specified by the table (perm). (*Id.* at col. 12:56-60.) Accordingly, Kocher2 does not disclose or suggest "executing said permutation operation on each of the first and second random values" (emphasis added), as recited in Applicant's claim 24.

Because Kocher1 and Kocher2 do not disclose the above-noted feature of Applicant's claim 24, these references, taken individually or in combination, cannot support a *prima facie* case for rejecting claim 24 under 35 U.S.C. § 103(a). Claim 24 is, therefore, allowable over Kocher1 and Kocher2. Claims 25-30 are also allowable at least due to their dependence from claim 24.

Independent claim 31, although of different scope than claim 24, recites subject matter similar to that recited in claim 24. For instance, claim 31 recites, *inter alia*, "executing said permutation operation on each of the first and second random values, to generate respective first and second random results." Accordingly, claim 31 is allowable over the applied references for the same reasons set forth above with regard to claim 24, and claims 32-37 are allowable at least due to their dependence from claim 31.

Conclusion

For the reasons set forth above, Applicant respectfully requests that prosecution of this Application be reopened and that the pending claims be allowed.

In the event that there are any questions concerning this paper, or the application in general, the Examiner is respectfully urged to telephone Applicant's undersigned representative so that prosecution of the application may be expedited.

If additional fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: January 16, 2008

By: /Steven L. Ashburn/
Steven L. Ashburn
Registration No. 56,636

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620